IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	Case No. 3:24-cr-00151
v.	)	
	)	JUDGE RICHARDSON
MATTHEW ISAAC KNOOT	)	

RESPONSE OF THE UNITED STATES TO THE COURT'S ORDER SEEKING SUPPLEMENTAL BRIEFING RELATED TO DEFENDANT'S MOTION TO SUPPRESS

Comes now the United States of America, by and through the undersigned Assistant United States Attorney, Joshua A. Kurtzman, and United States Department of Justice Trial Attorney Gregory J. Nicosia, Jr., and responds to the Court's May 6, 2025 Order (DE # 56), which directs the parties to answer three issues implicated by the arguments raised and relief sought in Defendant's Motion to Suppress (the "motion" or "motion to suppress"). (DE # 48.) First, even assuming *arguendo* the Premises Warrant ("Warrant 1") (DE # 48-1)[1] and the Discord Warrant (DE # 48-2) ("Warrant 2") (collectively, the "Warrants") are sufficiently particular, but nevertheless overly broad, *only* the portions of the Warrants determined to be overly broad should be invalidated; the rest of the Warrants (and the evidence collected pursuant to them) should not be suppressed. Second, again assuming *arguendo* that the Warrants are overly broad, Defendant's remedy is limited to severance of the portion of the Warrants that authorized the seizure of Defendant's *personal* digital devices and *personal* Discord account, but nothing else. Third, the *Leon* good faith exception specifically precludes the suppression of the evidence obtained pursuant to the Warrants, despite any purported issues with over breadth.

[1] Defendant's motion styled this warrant as a "Device Warrant," when, in reality, it is a premises warrant that authorized a search of defendant's residence, storage unit, and the digital devices within those areas. (*See* DE # 48-1 at pg. 20.) For clarity, the United States adopts the Court's labeling of this warrant as "Warrant 1."

PROCEDURAL BACKGROUND

On August 7, 2024, a Grand Jury in the Middle District of Tennessee indicted the Defendant, charging him in Count One with Conspiracy to Damage Protected Computers, in violation of Title 18, United States Code, Section 371; Count Two with Conspiracy to Commit Money Laundering, in violation of Title 18, United States Code, Section 1956(h); Count Three with Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code, Section 1349; Count Four with Intentional Damage to a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B), and (c)(4)(A)(i)(I); Count Five with Aggravated Identity Theft, in violation of Title 18, United States Code, Sections 1028(a)(1) and 2; and Count Six with Conspiracy to Cause the Unlawful Employment of Aliens, in violation of Title 18, United States Code, Section 371. (DE # 3.)

On October 4, 2024, the Defendant filed an unopposed motion to continue trial, which was granted on November 7, 2024. (DE # 16 and 29.) On February 17, 2025, the Defendant filed a second unopposed motion to continue trial, which was granted on February 18, 2025. (DE # 39 and 41.) Pursuant to the same order, trial was scheduled for June 24, 2025. *Id*. On April 1, 2025, the Defendant filed a motion to suppress. (DE # 48.) On April 14, 2025, the United States filed its response in opposition to Defendant's motion to suppress. (DE # 52.) On April 28, 2025, the Defendant filed his reply to the United States' response in opposition. (DE # 55.) On May 6, 2025, the Court issued the instant Order, which directed the parties to answer three discrete issues implicated by the arguments raised and relief sought in Defendant's motion to suppress. On May 9, 2025, the Defendant filed a third motion to continue trial over the United States' objection, which was granted on May 22, 2025. (DE # 58 and 70.) Pursuant to that order, trial was rescheduled for August 12, 2025. *Id.*

LAW AND ARGUMENT[2]

1. Even Assuming *Arguendo* the Warrants Are Overly Broad, Only the Portions of the Warrants Deemed to Be Overly Broad Should Be Invalidated.

In *United States v. Richards*, the Sixth Circuit observed that "[t]he cases on particularity are actually concerned with at least two rather different problems: one is whether the warrant supplies enough information to guide and control the agent's judgment in selecting what to take; and the other is whether the category as specified is too broad in the sense that it includes items that should not be seized." 659 F.3d 527, 537 (6th Cir. 2011) (quoting *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999) (citations and internal quotation marks omitted). Here, the Court asks the parties to focus on the latter issue, and specifically to what extent the Warrants are invalid if they are deemed overly broad. The Sixth Circuit has stated that "infirmity due to overbreadth does not doom the entire warrant; rather, it 'requires the suppression of evidence seized pursuant to that part of the warrant . . . , but does *not* require the suppression of *anything* described in the valid portions of the warrant (or lawfully seized-on plain view grounds, for example-during their execution).'" *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001) (quoting *United States v. Brown*, 984 F.2d 1074, 1077 (10th Cir.1993)) (emphasis added).

In determining what portions, if any, of a warrant are invalid, the Sixth Circuit has held that "the proper approach . . . is to sever the infirm portion of the search warrant from the remainder which passes constitutional muster. *United States v. Blakeney*, 942 F.2d 1001, 1027 (6th Cir. 1991). In *Blakeney*, the Sixth Circuit, citing approvingly of the Fifth Circuit, further noted that "'it would be harsh medicine indeed if a warrant which was issued on probable cause and which did particularly describe certain items were to be invalidated in toto merely because the affiant and the

[2] The United States has presented the issues herein as articulated by the Court in its May 6, 2025 Order; however, the United States does not concede that the Warrants are overly broad for the reasons set forth in its Response in Opposition to Defendant's Motion to Suppress. (DE # 52.)

magistrate erred in seeking and permitting a search for other items as well.'" *Id.* (quoting *United States v. Cook*, 657 F.2d 730, 735 (5th Cir. 1981) (internal citation omitted)). Thus, to the extent suppression is warranted, it is a narrow, fact-specific remedy.

In *Blakeney*, the defendant was arrested and his home searched as part of an investigation of a jewelry store robbery. 942 F.2d at 1008. There, the defendant argued that the warrant was overly broad because it did not describe with particularity the items to be searched for—in this case, jewelry—and seized, and specifically, that where the affiant had the ability to provide specific descriptions of the jewelry to be seized, the failure to do so rendered that portion of the warrant invalid. *Id*. at 1026. The specific language at-issue there was:

> Records, including travel documents showing travel to and from Wisconsin, motel records, telephone records, warehouse receipts and keys, clothing relating to the jewelry robbery; specifically, Nixon masks, rubber gloves, rectangular plastic containers, handguns, flex cuffs, air-conditioning duct tape, jewelers equipment, maps of Wisconsin, newspapers, walkie-talkies, and false identification *and jewelry*.

Id. (emphasis added). In applying the narrow, fact-specific remedy discussed above, the Sixth Circuit held that the use of the generic term "jewelry," was overbroad, particularly where an inventory of the items taken during the jewelry store robbery was available to the affiant of the search warrant. *Id.* at 1027. This did not, however, render *any* other items in the same list constitutionally infirm. *See id.* Indeed, the Court noted that "[u]se of a generic term or generic description is not a per se violation of the Fourth Amendment." *Id.* Instead, the degree of specificity required is "flexible and will vary depending on the crime involved and the types of items sought." *United States v. Ables*, 167 F.3d 1021, 1033 (6th Cir. 1999).

Based on the foregoing, to the extent the Court finds some portion of the Warrants to be invalid due to overbreadth—which the United States does not concede—this Circuit's

precedent requires the Court to excise only those portions of the warrant with precision, leaving intact the remainder of the Warrants.

2. Even Assuming *Arguendo* that the Warrants Are Overly Broad, Defendant's Remedy Is Limited to Severance of the Portion of the Warrants that Authorized the Seizure of His Personal Digital Devices and the Fruits Thereof.

As it relates to Warrant 1, Defendant argues it is overly broad because "it does not identify with particularity which 'digital devices' are subject to seizure." (DE # 48 at 8.) Attachment B of Warrant 1 sets forth five categories of "items, information, and data to be seized" relating to violations of 18 U.S.C. §§ 1028 and 1030, one of which relates to digital devices:

> d. Electronic equipment, such as computers, personal organizers, personal digital assistant (PDA), telex machines, facsimile machines, currency counting machines, pagers, telephone answering machines and related manuals used to generate, transfer, count, record and/or store information.

(DE # 48-1 at Attachment B.) This subparagraph provides a list of various digital devices contextualized by the introductory paragraph—which narrows the scope of Warrant 1 to items, information, and data relating to violations of 18 U.S.C. §§ 1028 and 1030—and the affidavit itself. Unlike *Blakeney*, the level of specificity of the items in this subparagraph are about the same; therefore, it would be challenging to conclude whether or not this subparagraph passes muster devoid of additional context. That is, there are not some list items with more detailed descriptions than others, as there were in *Blakeney*, which could resolve the issue as it did in that case. Thus, because a generic term or generic description is not a per se invalid under the Fourth Amendment, we must then view this subparagraph in light of the *specific* crimes and information sought; context which is provided by the affidavit and described at length in the United States'

Response in Opposition to the instant Motion to Suppress. *Blakeney*, 942 F.2d at 1027; (*see also* DE # 52 at 9-17.).

However, the Court directs us to consider the scope of Defendant's remedy, assuming *arguendo*, that Warrant 1 is indeed overly broad. Here, the result would be somewhat different than the cases discussed above because the Court would not be excising a generic word or phrase to remove the constitutional infirmity. Instead, it would be reading a limitation into the warrant: that Warrant 1 should *only* apply to *third-party* digital devices, rather than *personal* devices. Defendant concedes Warrant 1 clearly establishes case-specific facts to search and seize company-issued laptops. (DE # 48 at 3.) Presumably, this limitation would be based on the purported absence of an unequivocal connection between the Defendant's personal devices and the subject offenses. The consequence of this limitation would be a straightforward application of the doctrine that "infirmity due to overbreadth does not doom the entire warrant. *Greene*, 250 F.3d at 477 (quoting *United States v. Brown*, 984 F.2d 1074, 1077 (10th Cir.1993). Here, it would preserve the other digital and documentary evidence seized from Defendant's home, while suppressing only the information from Defendant's personal devices.[3]

Assuming *arguendo* that the portion of Warrant 1 relating to Defendant's personal devices is overly broad, the Court next asks the parties to consider what effect, if any, this has on Warrant 2. Warrant 2 relates much of the same factual basis as Warrant 1. (*See* DE # 48-2 at ¶¶ 7-15.) It further states that an analysis of Defendant's desktop computer yielded chat messages between the Defendant and co-conspirator Yang Di via the encrypted communication platform Discord. (*Id.* at

[3] During the search, agents seized, among other things, seven laptops, three tablets, seven cell phones, six external hard drives, one internal hard drive, one custom desktop computer, one "mouse jiggler," one cardboard box with shipping label addressed to A. M., and postal receipt(s). As noted above, Defendant's Motion is primarily concerned with the custom desktop computer, which was later determined to be Defendant' personal computer.

¶ 16.) Those messages revealed, among other things, that Yang Di offered to pay the Defendant to receive laptops; that the Defendant agreed to receive laptops in exchange for a fee (that he re-negotiated); that Yang Di would interview for remote IT work positions; that Yang Di obtained at least two jobs; and that Defendant would assist Yang Di with onboarding, including completing I-9 and W4 forms. (*Id*.) Warrant 2 further states that at least one of the Discord accounts was registered to an email address controlled by the Defendant. (Id. at ¶¶ 15, 16.)

Overbreadth in the context of a search warrant that authorizes the search of electronic evidence creates a "unique problem" given the "practical difficulties inherent in implementing universal search methodologies." *Richards*, 659 F.3d at 538. With respect to searches of computers, the Sixth Circuit adopted the standard articulated in *United States v. Burgess*, which held, in brief, that "[w]hile officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant, . . . a computer search may be as extensive as reasonably required to locate the items described in the warrant based on probable cause." *Id*. (quoting *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir.), cert. denied, 558 U.S. 1097 (2009) (citations and internal quotation marks omitted)). As noted in the Unites States' Response in Opposition, in applying a reasonableness analysis on a case-by-case basis, the Sixth Circuit has rejected most particularity challenges to warrants authorizing the search of entire personal or business computers. *Id*. at 539 (citing *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir.2001) (rejecting particularity challenge to the seizure and off-site search of entire computers and their contents in an obscenity investigation because "the warrants required that the communications and computer records pertain to the listed offenses" and "[d]efendants could not have obtained more specific identification of e-mails and subscriber data, which were not accessible to them" and reasoning that "[a]lthough there were presumably communications on

the computers that did not relate to the offenses, '[a] search does not become invalid merely because some items not covered by a warrant are seized.'"); *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988) (rejecting a Fourth Amendment challenge to the seizure of documents and computer files that were unrelated to the offenses because the Sixth Circuit concluded that it would have been unreasonable to require police to sort through extensive files in a suspect's office in order to separate out those items that were outside the warrant.).

As the Court's Order recognizes, there are several potential permutations to this analysis. (DE # 56 at 3.) Beginning with the applicable law, we must apply the two principles discussed above. First, the Court must apply the reasonableness analysis on a case-by-case basis analysis applied to searches of digital data, recognizing, of course, that it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in order to determine whether they contain such evidence." *Richards*, 659 F.3d at 540. Second, the Court must then only "sever the infirm portion of the search warrant from the remainder which passes constitutional muster." *Blakeney*, 942 F.2d at 1027.

Confined to the four corners of Warrant 2, the Court could reasonably conclude that Warrant 2 is *not* overly broad. Indeed, the specific information in Attachment B of Warrant 2 is "as extensive as reasonably required to locate the items described in the warrant based on probable cause." *Richards*, 659 F.3d at 538. While each category of information may seem overly broad out of context, the information sought was reasonably necessary to determine who was in control of these Discord accounts, what their role in the conspiracy was, and their true identities, among other things. For example, list items (a) and (c) seek basic subscriber information for the accounts, the date of creation, and IP address used on the date of creation, which is relevant to determining who owns or controls the accounts, their locations, and additional identifiers that could be used to locate

them. List items (b) and (f) seek all past and current usernames and data associated with their profile pages, which is relevant to determining who owns or controls the accounts, as well as the potential use of these accounts in other related crimes. List items (d) and (g) seek all internet protocol log information and other relevant log information, which establishes what devices were used to access these accounts, the potential location of the users of these accounts, and their language preferences, among other things. Finally, list item (h) requests all chat messages associated with the accounts, which is relevant because the investigators knew that the co-conspirators planned at least some aspects of the offenses under investigation via Discord. Thus, each category of information was reasonably calculated to locate information responsive to the warrant. The mere fact that each category requested "all" information for each of the nine categories does not render it invalid. Indeed, this demonstrates the "unique problem" that caused the *Richards* Court to adopt an approach that balances Defendant's constitutional rights against the difficulties inherent to searching computers and other electronic data.

However, if we assume *arguendo* the Court's ruling with respect to Warrant 1 applies to Warrant 2, we must then excise from Warrant 2 the information obtained from Defendant's personal devices, which includes the Discord messages discovered on Defendant's desktop. (DE # 48-2 at ¶ 16.) This would almost certainly render Warrant 2 invalid in regard to Defendant's Discord account because the new information serving as the basis of the search requested in Warrant 2—the Discord chats on Defendant's computer—would be stricken. *See Blakeney*, 942 F.2d at 1027.

Even so, there remains one further permutation that was first raised in the United States' Response in Opposition to Defendant's Motion to Suppress: whether the Defendant has standing to challenge the portion of the Warrant 2 relating to his co-conspirator's account. (DE # 52 at 25-

26.) Attachment B of Warrant 2 sets forth nine discrete categories of information to be disclosed to the United States relating to four identifiers: Discord user ID 913420784490405908, username yangdi0027, username mellamomateo, and email address matthewknoot@tutanota.com. Thus, if the Defendant lacks standing to challenge the portion of the Warrant 2 returns related to the yangdi0027 account, that information should *not* be suppressed. Here, we read the principles articulated in *Richards* and *Blakeney*, along with the generally accepted principles of the standing doctrine, together to yield this result. If the Defendant lacks standing to challenge the portion of Warrant 2 relating the yangdi0027 account (and fruits thereof)—but is otherwise successful is challenging Warrant 2 on the grounds that it relies on the purportedly overly broad fruits of Warrant 1—it follows that *only* the portions relating to *Defendant's* Discord account should be severed. This is consistent with the Sixth Circuit's precedent that, to the extent suppression is warranted, it is a narrow, fact-specific remedy. *See Blakeney*, 942 F.2d 1001, 1027 (6th Cir. 1991).

3. The *Leon* Good Faith Exception Precludes the Suppression of the Evidence Even if the Court Finds the Warrants Constitutionally Deficient Due to Overbreadth.

As noted in the United States Response in Opposition to Defendant's Motion to Suppress, even if the Warrants were defective—which they are not—the Defendant's motion still fails under the *Leon* good-faith exception. As the Sixth Circuit has noted, even if a search warrant is defective, district courts shall not suppress evidence seized pursuant to such warrant if the seizure was based on reasonable, good faith reliance on the warrant, which is the case here. *United States v. Frazier*, 423 F.3d 526, 533 (6th Cir.2005) (citing *United States v. Leon*, 468 U.S. 897, 905 (1984)). The Supreme Court explained the mechanics of the good faith exception:

> [O]ur good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization. In making this determination, all of the circumstances—including whether the warrant application had previously been rejected by a different magistrate—may be considered.

Leon, 468 U.S. at 922–23 n. 23.

The rationale behind the exception is that the exclusionary rule is meant to deter unlawful police conduct. *United States v. Abboud*, 438 F.3d 554, 578 (6th Cir. 2006). This policy of deterrence is not served by the exclusion of evidence seized in good faith by the police. *Id.* (citing *Leon*, 468 U.S. at 918–19). The only instances where the good faith exception does not apply are in the following specific circumstances: "1) the supporting affidavit contained knowing or reckless falsity; 2) the issuing magistrate wholly abandoned his or her judicial role; 3) the affidavit is 'so lacking in probable cause as to render official belief in its existence entirely unreasonable;' or 4) where the officer's reliance on the warrant was neither in good faith nor objectively reasonable." *Frazier*, 423 F.3d at 533 (quoting *Leon*, 468 U.S. at 923). Finally, the government bears the burden of showing that law enforcement obtained the evidence in "reasonable, good-faith reliance" on a defective search warrant. *United States v. Ward*, 967 F.3d 550, 554 (6th Cir. 2020) (citation omitted).

These general principles remain true even where the underlying warrant is determined to be overly broad. Here, *United States v. Schultz*, which discussed the good faith exception in relation to a search warrant with a nexus problem, is instructive.[4] 14 F.3d 1093 (6th Cir. 1994). In *Schultz*, the Sixth Circuit found the warrant under review failed to make "any material connection between" the safe deposit box which was searched and any criminal activity. *Id.* at 1097. "Nevertheless, under current Supreme Court doctrine, the district court was correct to deny the Motion to Suppress, because the first warrant comes under the so-called 'good faith' exception…". *Id.* at 1098. There, the Sixth Circuit applied the four factors set forth in *Frazier* (discussed above) and concluded that the warrant should not be suppressed. *Id.*

[4] Both parties discussed *Schultz* at length in their prior filings. (*See* DE # 48 at 10-13 and DE # 52 at 21-22.)

Here, it is without doubt that the government acted in "reasonable, good-faith reliance" on warrants issued by a neutral magistrate. *Ward*, 967 F.3d at 554. First, the Defendant's motion does not argue, and there are not facts to suggest, that the affidavit contained any "knowing or reckless falsity." *Frazier*, 423 F.3d at 533. Second, both Warrants were drafted by Special Agent Rousseau and then reviewed by the Department of Justice in the normal course. Both Warrants were then presented to the same Magistrate Judge, the Hon. Barbara D. Holmes, who reviewed and approved them. Notably, Judge Holmes approved Warrant 2 *knowing* that it relied on the fruits of Warrant 1. Thus, if there had been some concern about the seizure of evidence from Defendant's personal digital devices, Judge Holmes could have raised that issue with the government. Instead, she authorized Warrant 2. Taken together, Agent Rousseau's reliance on the warrants was neither objectively unreasonable, nor in bad faith because a sitting Magistrate Judge, who was familiar with the facts of the investigation, reviewed and approved both Warrants. Third and finally, both Warrants outline a sufficient factual basis to establish that probable cause existed to believe that computer fraud and identity theft crimes occurred, the Defendant was involved, the Defendant had computers and devices associated with the fraud scheme at his residence, and the Defendant used his Discord account to further the criminal conspiracy.

With respect to this final prong of the analysis—whether the affidavit was so lacking in probable cause as to render official belief in its existence entirely unreasonable—*United States v. Ward* provides is a helpful comparison. In *Ward*, the Sixth Circuit explained that an affidavit "'so lacking in indicia of probable cause'" is known as a "'bare bones'" affidavit. *Ward*, 967 F.3d at 554 (quoting *United States v. White*, 874 F.3d 490, 496 (6th Cir. 2017)). To avoid being labeled a "bare bones" affidavit, it must state more than "suspicions, or conclusions, without providing some underlying factual circumstances regarding veracity, reliability, and basis of knowledge" and make

"some connection" between the illegal activity and the place to be searched. *Id*. (internal citations omitted). Here, both Warrants easily pass this test.

The Warrant 1 affidavit states the FBI confirmed three separate companies had hired an individual purporting to be A.M. and shipped laptops to the same address, where Defendant was the resident. (DE # 48-1 ¶¶ 17, 20-21.) The FBI had also confirmed that at least one of those victim company devices had connected to its network from a Chinese internet protocol address, using technology designed to obscure the end-user(s)' true location and identity. (*Id*. at ¶ 17.) Thus, at a minimum, there was probable cause to believe that digital devices were used in furtherance of identity theft and computer fraud. Similarly, Warrant 2 restated all of the above information and further provided verbatim reproductions of Discord chats taken from Defendant's computer, thereby establishing the use of Discord by the Defendant in furtherance of the crimes under investigation. By contrast, in *Ward* the affidavit provided: (1) undated text messages indicating that Ward sold someone else heroin and crack-cocaine; (2) that sixth month's later police found an unidentified quantity of loose marijuana, cigar wrappers, and a plastic bag containing residue of an unidentified substance in Ward's trash; and (3) that Ward was previously charged, but not convicted, with drug and weapons offenses. *Ward*, 967 F.3d at 554. Based on the foregoing, both Warrants were sufficiently detailed such that it was reasonable for a neutral and detached magistrate—who was familiar with the investigation—to issue them. Accordingly, should the Court find that the Warrants are overly broad—which they are not—the *Leon* good faith exception applies, and none of the evidence obtained pursuant to Warrant 1 or Warrant 2 should be suppressed.

CONCLUSION

Based on the foregoing, the United States respectfully submits that the Court should deny the defendant's Motion to Suppress and do so without an evidentiary hearing.

Respectfully submitted,

ROBERT E. MCGUIRE
Acting United States Attorney

By: *s/ Joshua A. Kurtzman*

JOSHUA A. KURTZMAN
Assistant U. S. Attorney
719 Church Street - Suite 3300
Nashville, Tennessee 37203-3870
Telephone: 615-401-6617

s/ Gregory Jon Nicosia, Jr.

GREGORY JON NICOSIA, JR.
D.C. Bar No. 1033923
Trial Attorney
National Security Division
950 Pennsylvania Avenue, NW
Washington, DC 20530
(202) 353-4273
Gregory.Nicosia@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that the above document was filed through the ECF system and will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

Date: May 30, 2025

/s/ Gregory Jon Nicosia, Jr.
GREGORY JON NICOSIA, JR.
Trial Attorney
National Security Division